IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

UTILITY PATENT APPLICATION

FOR

METHOD AND APPARATUS FOR TRANSITIONING BETWEEN STATES OF SECURITY POLICIES USED TO SECURE ELECTRONIC DOCUMENTS

Inventors: Klimenty Vainstein
Satyajit Nath
Michael Michio Ouye

Assignee: PSS Systems, Inc.

METHOD AND APPARATUS FOR TRANSITIONING BETWEEN STATES OF SECURITY POLICIES USED TO SECURE ELECTRONIC DOCUMENTS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is related to: (i) U. S. Patent Application No.: _____ (Att.Dkt.No. SSL1P020), filed concurrently herewith, and entitled "METHOD AND SYSTEM FOR SECURING DIGITAL ASSETS USING PROCESS-DRIVEN SECURITY POLICIES," which is hereby incorporated herein by reference; (ii) U. S. Patent Application No.: 10/405,587, filed April 1, 2003, and entitled "METHOD AND APPARATUS FOR SECURING DIGITAL ASSETS USING CONTENT TYPE DESIGNATIONS," which is hereby incorporated herein by reference; (iii) U. S. Patent Application No.: 10/159,537, filed May 5, 2002, and entitled "METHOD AND APPARATUS FOR SECURING DIGITAL ASSETS," which is hereby incorporated herein by reference; and (iv) U. S. Patent Application No.: 10/127,109, filed April 22, 2002, and entitled "EVALUATION OF ACCESS RIGHTS TO SECURED DIGITAL ASSETS," which is hereby incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The present invention relates to security systems for data and, more particularly, to security systems that protect data in an inter/intra enterprise environment.

Description of Related Art

[0003] The Internet is the fastest growing telecommunications medium in history. This growth and the easy access it affords have significantly enhanced the opportunity to use advanced information technology for both the public and private sectors. It provides unprecedented opportunities for interaction and data sharing among businesses and individuals. However, the advantages provided by the Internet come with a significantly greater element of risk to the confidentiality and

integrity of information. The Internet is an open, public and international network of interconnected computers and electronic devices. Without proper security means, an unauthorized person or machine may intercept information traveling across the Internet and even gain access to proprietary information stored in computers that interconnect to the Internet.

[0004] There are many efforts in progress aimed at protecting proprietary information traveling across the Internet and controlling access to computers carrying the proprietary information. Cryptography allows people to carry over the confidence found in the physical world to the electronic world, thus allowing people to do business electronically without worries of deceit and deception. Every day millions of people interact electronically, whether it is through *e*-mail, *e*-commerce (business conducted over the Internet), ATM machines, or cellular phones. The perpetual increase of information transmitted electronically has led to an increased reliance on cryptography.

[0005] One of the ongoing efforts in protecting the proprietary information traveling across the Internet is to use one or more cryptographic techniques to secure a private communication session between two communicating computers on the Internet. The cryptographic techniques provide a way to transmit information across an unsecure communication channel without disclosing the contents of the information to anyone eavesdropping on the communication channel. Using an encryption process in a cryptographic technique, one party can protect the contents of the data in transit from access by an unauthorized third party, yet the intended party can read the encrypted data after using a corresponding decryption process.

[0006] A firewall is another security measure that protects the resources of a private network from users of other networks. However, it has been reported that many unauthorized accesses to proprietary information occur from the inside, as opposed to from the outside. An example of someone gaining unauthorized access from the inside is when restricted or proprietary information is accessed by someone within an organization who is not supposed to do so. Due to the open nature of networks, contractual information, customer data, executive communications, product specifications, and a host of other confidential and proprietary intellectual property remain available and vulnerable to improper access and usage by unauthorized users within or outside a supposedly protected perimeter.

[0007] Many businesses and organizations have been looking for effective ways to protect their proprietary information. Typically, businesses and organizations have deployed firewalls, Virtual Private Networks (VPNs), and Intrusion Detection Systems (IDS) to provide protection. Unfortunately, these various security means have been proven insufficient to reliably protect proprietary information residing on private networks. For example, depending on passwords to access sensitive documents from within often causes security breaches when the password of a few characters long is leaked or detected. Consequently, various cryptographic means are deployed to provide restricted access to electronic data in security systems.

[0008] Various security criteria, such as encryption or decryption keys, are often used to facilitate restricted access to data in security systems. Conventional uses of security criteria provide static assignment of security criteria to electronic resources being secured. However, the assigning of security criteria in a static manner does not permit subsequent alteration of the security criteria under certain conditions. Although an administrator may be able to change the security criteria for an electronic resource that has already been secured, such alteration would be a manual process only available to the administrator. Further, given that an administrator is managing secure electronic resources (e.g., data) for many users, it is not feasible for the administrator to participate in the changing of security criteria for a large volume of electronic resources. Therefore, there is a need to provide more effective ways for security systems to permit security criteria imposed on electronic resources to be changed, thereby altering the security used to protect the electronic resources.

SUMMARY OF THE INVENTION

[0009] The invention relates to techniques for dynamically altering security criteria used in a system (e.g., a file security system for an enterprise). The security criteria pertains to keys (or ciphers) used by the file security system to encrypt electronic files to be secured, or to decrypt electronic files already secured. The security criteria can, among other things, include keys that are required to gain access to electronic files. Here, the keys can be changed automatically as electronic files transition between different states of a process-driven security policy. The dynamic

alteration of security criteria enhances the flexibility and robustness of the security system. In other words, access restrictions on electronic files can be dependent on the state of the process-driven security policy and enforced in conjunction with one or more cryptographic methods.

[0010] According to one aspect of the invention, methods and systems for securing electronic files use process-driven security policies. As an electronic file transitions through a process, access restrictions can automatically change. The process can be defined by a number of states, with each state having different security policies associated therewith. The security policies control, for example, which users are permitted to access the electronic files, or how the electronic files can be accessed. In one embodiment, the access restrictions are imposed by one or more keys that are required to decrypt electronic files that were previously secured. The process can also be referred to as a workflow, where the workflow has a series of states through which files (documents) can move, where different security policies can be imposed at different states.

[0011] Another aspect of the invention is that process-driven security policies are enforced or controlled at a server of a file security system. A group of one or more electronic documents are bound together and progress together through states of a process specified by process-driven security policies. The server can automatically and remotely enforce the process-driven security policies on the group of electronic documents.

[0012] Still another aspect of the invention is that process-driven security policies are controlled at a client of a file security system. Here, each individual electronic document can be separately and independently bound to process-driven security policies. The process-driven security policies can thus operate at the client with little or no communication with a central server in most cases.

[0013] The process-driven security policies typically offer persistent states. Each state can specify a different set of users or groups of users that are permitted access to an electronic document. The states are also independent of the electronic documents themselves.

[0014] The invention can be implemented in numerous ways, including as a method, system, device, and computer readable medium. Several embodiments of the invention are discussed below.

[0015] As a document security system for restricting access to documents, one embodiment of the invention includes at least: a process-driven security policy that includes a plurality of states and transition rules, each of the states corresponding to one or more access restrictions, and the transition rules specify when the secured document is to transition from one state to another; and an access manager that determines whether access to a secured document is permitted by a requestor based on the state and the corresponding one or more access restrictions thereof for the process-driven security policy.

[0016] As a method for transitioning at least one secured document through a security-policy state machine having a plurality of states, one embodiment of the invention includes at least the acts of: receiving an event; determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent state of the security-policy state machine; and automatically transitioning from the former state to the subsequent state of the security-policy state machine when the determining determines that the event causes the state transition.

[0017] As a method for imposing access restrictions on electronic documents, one embodiment of the invention includes at least the acts of: providing at least one process-driven security policy at a server machine, the process-driven security policy having a plurality of states associated therewith, each of the states having distinct access restrictions; providing a reference to the process-driven security policy at a client machine, the reference referring to the process-driven security policy resident on the server machine; associating the reference to an electronic document; transitioning the process-driven security policy from one state to a current state; and subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy, the current state being informed to the server computer by sending the reference to the server computer.

[0018] As a computer readable medium including at least computer program code for transitioning at least one secured document through a security-policy state

machine having a plurality of states, one embodiment of the invention includes at least: computer program code for receiving an event; computer program code for determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent state of the security-policy state machine; and computer program code for automatically transitioning from the former state to the subsequent state of the security-policy state machine when the computer program code for determining determines that the event causes the state transition.

[0019] As a computer readable medium including at least computer program code for imposing access restrictions on electronic documents, one embodiment of the invention includes at least: computer program code for providing at least one process-driven security policy at a server machine, the process-driven security policy having a plurality of states associated therewith, each of the states having distinct access restrictions; computer program code for providing a reference to the process-driven security policy at a client machine, the reference referring to the process-driven security policy resident on the server machine; computer program code for associating the reference to an electronic document; computer program code for transforming the process-driven security policy from one state to a current state; and computer program code for determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy, the current state being informed to the server computer by sending the reference to the server computer.

[0020] Other objects, features, and advantages of the present invention will become apparent upon examining the following detailed description of an embodiment thereof, taken in conjunction with the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] These and other features, aspects, and advantages of the invention will become better understood with regard to the following description, appended claims and accompanying drawings, wherein:

[0022] FIG. 1 is a diagram of an exemplary process-driven security policy (PDSP) according to one embodiment of the invention.

[0023] FIG. 2 is a flow diagram of a transition process according to one embodiment of the invention.

[0024] FIG. 3 illustrates a security policy state machine according to one embodiment of the invention.

[0025] FIG. 4A is a diagram of a document securing system according to one embodiment of the invention.

[0026] FIG. 4B is a flow diagram of a document securing process according to one embodiment of the invention.

[0027] FIG. 4C is a detailed flow diagram of an encryption process according to one embodiment of the invention.

[0028] FIG. 5A is a diagram of a document unsecuring system according to one embodiment of the invention.

[0029] FIGs. 5B and 5C are flow diagrams of a document access process according to one embodiment of the invention.

[0030] FIG. 5D is a flow diagram of a decryption process according to one embodiment of the invention.

[0031] FIG. 6 is a flow diagram of a transition process according to one embodiment of the invention.

[0032] FIG. 7 shows a basic security system in which the invention may be practiced in accordance with one embodiment thereof.

[0033] FIG. 8 shows an exemplary data structure of a secured file that may be used in one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0034] The invention relates to techniques for dynamically altering security criteria used in a system (e.g., a file security system for an enterprise). The security criteria pertains to keys (or ciphers) used by the file security system to encrypt electronic files to be secured, or to decrypt electronic files already secured. The security criteria can, among other things, include keys that are required to gain access to electronic files. Here, the keys can be changed automatically as electronic files

transition between different states of a process-driven security policy. The dynamic alteration of security criteria enhances the flexibility and robustness of the security system. In other words, access restrictions on electronic files can be dependent on the state of the process-driven security policy.

[0035] As used herein, a file may include, but not be limited to, one or more various types of documents, multimedia files, data, executable code, images and texts, and in some cases, a collection of files. Accordingly, a secured file means that an electronic file typically stored or presented in a form that is nearly impossible to read without authorization and authentication. Its purpose is to ensure privacy by keeping the content in a file hidden from anyone for whom it is not intended, even those who may have a copy of the file.

[0036] According to one aspect of the invention, methods and systems for securing electronic files use process-driven security policies. As an electronic file transitions through a process, access restrictions can automatically change or remain intact depending on the process. The process can be defined by a number of states, with each state having its corresponding security policies associated therewith. The security policies control, for example, which users are permitted to access the electronic files or how the electronic files can be accessed. In one embodiment, the access restrictions are imposed by one or more keys that are required to decrypt electronic files that were previously secured. The process can also be referred to as a workflow, where the workflow has a series of states through which files (documents) can move, where different security policies can be imposed at different states.

[0037] Another aspect of the invention is that process-driven security policies are controlled at a server of a file security system. A group of one or more electronic documents are bound together and progress together through states of a process specified by process-driven security policies. The server can automatically and remotely enforce the process-driven security policies on the group of electronic documents.

[0038] Still another aspect of the invention is that process-driven security policies are controlled at a client of a file security system. Here, each individual electronic document can be separately and independently bound to process-driven security

policies. The process-driven security policies can thus operate at the client with little or no communication with a central server.

[0039] The process-driven security policies typically offer persistent states. Each state can specify a different set of users that are permitted access to an electronic document. The states are also independent of the electronic documents themselves.

[0040] Secured files are files that require one or more keys, passwords, access privileges, etc. to gain access to their content. The security is often provided through encryption and access rules. The files, for example, can pertain to documents, multimedia files, data, executable code, images and text. In general, a secured file can only be accessed by authenticated users with appropriate access rights or privileges. In one embodiment, each secured file is provided with a header portion and a data portion, where the header portion contains, or points to, security information. The security information is used to determine whether access to associated data portions of secured files is permitted.

[0041] In one embodiment, security information provided with an electronic document controls restrictive access to a data portion which is encrypted. The security information can employ access rules together with cipher keys (e.g., a file key and various other keys) to ensure that only those users with proper access privileges or rights can access the encrypted data portion.

[0042] As used herein, a user may mean a human user, a software agent, a group of users, a member of the group, a device and/or application. Besides a human user who needs to access a secured document, a software application or agent sometimes needs to access secured files in order to proceed. Accordingly, unless specifically stated, the "user" as used herein does not necessarily pertain to a human being.

[0043] The invention is related to processes, systems, architectures and software products for providing pervasive security to digital assets (e.g., electronic documents). The invention is particularly suitable in an enterprise environment. In general, pervasive security means that digital assets are secured (i.e., secured data) and can only be accessed by authenticated users with appropriate access rights or

privileges. Digital assets may include, but not be limited to, various types of documents, multimedia files, data, executable code, images and texts.

[0044] In the following description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will become obvious to those skilled in the art that the invention may be practiced without these specific details. The description and representation herein are the common meanings used by those experienced or skilled in the art to most effectively convey the substance of their work to others skilled in the art. In other instances, well-known methods, procedures, components, and circuitry have not been described in detail to avoid unnecessarily obscuring aspects of the invention.

[0045] Reference herein to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment can be included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Further, the order of blocks in process flowcharts or diagrams representing one or more embodiments of the invention do not inherently indicate any particular order, nor imply any limitations in the invention.

[0046] Embodiments of the invention are discussed herein with reference to FIGs. 1 – 8. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes as the invention extends beyond these limited embodiments.

[0047] FIG. 1 is a diagram of an exemplary process-driven security policy (PDSP) 100 according to one embodiment of the invention. The process-driven security policy 100 includes a plurality of different states. As shown in FIG. 1, the process-driven security policy 100 can include state A 102, state B 104, state C 106, and state D 108. Each of these different states can be associated with one or more access restrictions.

[0048] The process-driven security policy 100 is used by a file (document) security system to restrict access to files (documents). As files are placed in different ones of the states of the process-driven security policy 100, the access

restrictions being utilized to secure access to the files typically changes. More particularly, as the files move from state-to-state in accordance with a process, the access restrictions utilized by the files often changes. Indeed, the access restrictions can change automatically based upon the state the file is in, and thus does not necessarily require user or administrator interaction in order to change the access restrictions. Typically, access restrictions will designate which users (or groups of users) are able to access secure documents, whether certain clearance levels are needed, whether off-line access is permitted, and which of various other possible criteria or considerations are utilized. A set of access restrictions for the various states can be referred to as a security policy.

[0049] A file can transition between the various states of the process-driven security policy 100 in a controlled manner. Often, the process-driven security policy 100 defines the transitions that are permissible. In one embodiment, the state transitions are event-driven. The events can be either internal to the file security system or external to the file security system. When event-driven, the transitions between states can be automatic and thus do not require user or administrator interaction. However, some events can be triggered or initiated by user or administrator interaction.

[0050] As shown in FIG. 1, a file (document) can transition between the different states 102-108 offered by the process-driven security policy 100. For example, a file currently in state A 102 can transition to state B 104 or state D 108, depending upon process-related conditions (e.g., events). Similarly, a file in state D 108, depending upon process considerations, can transition to state A 102, state B 104 or state C 106. Likewise, a file in state B 104 or state C 106 can transition to one or more other states. Additional details on states, security policies and transitions between states are discussed in additional detail below.

[0051] FIG. 2 is a flow diagram of a transition process 200 according to one embodiment of the invention. The transition process 200 can be used to transition a document (file) between different states of a process-driven security policy, such as the process-driven security policy shown in FIG. 1. The transition process 200 is typically deemed process-driven because it is driven by a process. The process is, for example, defined by transition rules. The transition rules typically rely upon events to cause transitions between states. Often user or administrator interaction is

not involved when activating transitions. However, the transition process 200 can permit a user or administrator to participate in activating transitions, such as by causing an event to occur which initiates a transition.

[0052] The transition process 200 begins with a decision 202 that determines whether an event relevant to the process-driven security policy imposed on a document has been received. Typically, the process-driven security policy is imposed on the document by a file security system. One implementation of a process-driven security policy is a security policy state machine. The process-driven security policy (or security policy state machine) has a plurality of states, and transition rules for transitioning between the various states. In any case, the transition process 200 monitors events that are relevant to the process-driven security policy (or the security policy state machine). When the decision 202 determines that an event has not yet been received, the transition process 200 awaits such an event.

[0053] On the other hand, when the decision 202 determines that an event has been received, then the transition process 200 determines 204 whether the event causes a state transition. Here, the rules by which transitions between states occur, i.e., transition rules, can be specified by the process-driven security policy. For example, an administrator for the document security system may have created the process-driven security policy and thus defined its states and its transition rules. Hence, when an event is received, it is evaluated to determine 204 whether the event causes a state transition. When the decision 206 determines that a state transition is to occur, the state transition is performed 208 to transfer one or more documents from one state to another state. Alternatively, when the decision 206 determines that a state transition is not to occur, the block 208 is bypassed so that no state transition is performed. Once the one or more documents transition to the new state, the access restrictions for the new state govern when access to the documents, which are secured, is permitted. Following the block 208 or its being bypassed, the transition process 200 is complete and ends.

[0054] FIG. 3 illustrates a security policy state machine 300 according to one embodiment of the invention. As previously noted, a security policy state machine is one implementation of a process-driven security policy. In this exemplary embodiment, the security policy state machine 300 includes four distinct states,

namely, a state A ("Draft") 302, state B ("Final Draft") 304, state C ("Retain") 306, and state D ("Delete") 308. Each of these states has one or more associated access restriction for documents (files) which reside in that state. Further, the permitted transitions between the various states 302-308 are identified by transitions T1- T5. In particular, a document in the Draft state 302 can follow the transition T1 to the Final Draft state 304. A document in the Final Draft state 304 can follow the transition T2 to the Retain state 306. A document in the Retain state 306 can follow transition T3 to the Delete state 308. Further, a document in the Final Draft state 304 can follow transition T4 to the Draft state 302, and a document in the Retain state 306 can follow transition T5 to the Final Draft state 304.

[0055] A file security system can enforce the security policy state machine 300 on one or more electronic documents. In doing so, the security policy state machine 300 is typically described in a textual manner, such as in a markup language (e.g., XML), pseudo-code, and the like. One representative example of a textual description of the security policy state machine 300 is as follows.

```
State=DRAFT
Accessors = Finance, unrestricted
Deny off-line access
Grant audit access

State=FINAL DRAFT
Accessors = Finance, restricted; Finance Managers, unrestricted
Deny off-line access
Grant audit access

State=RETAIN
Accessors = All
Allow off-line access
Deny audit access

State=DELETE
Accessors = None
```

[0056] Note that in the Draft state, the users with permission to access the electronic document (referred to as "Accessors") include those users that are members of a Finance group. The access is also unrestricted in this Draft state. Also, in the Draft state, offline access to the electronic document is not permitted, but audit access is permitted. Note, however, in the Final Draft state, those users that

are members of the Finance group now only have restricted access. In one embodiment, restricted access means that the data (content) of the document can be accessed but that such data cannot be further disseminated through operations such as cut, paste, print, etc.

[0057] Additionally, the security policy state machine 300 transitions between the various states in accordance with transition rules. Typically, the transition rules are triggered by the occurrence of events. The events can be internal or external. The external events can originate from users or from another system (e.g., a document management system). In a specific case of the security policy state machine 300, a representative description of a transition rule is as follows.

On event (), transition from STATE1 to STATE2

[0058] Some exemplary transition rules using internal or external events are as follows.

On (time = September 1, 2008), RETAIN to DELETE

On (ExtEvent == docCheckIn), FINAL DRAFT to RETAIN

On (ExtEvent == docFinalize), DRAFT to FINAL DRAFT

On (ExtEvent == docReject), FINAL DRAFT to DRAFT

On (period = event transition day (FINAL DRAFT) + 90 days), FINAL DRAFT to RETAIN

[0059] Of these exemplary transition rules, the first and last transition rules are triggered by internal events and the others are triggered by external events. For example, the external events can be from a document management system that is separate from the file (document) security system.

[0060] FIG. 4A is a diagram of a document securing system 400 according to one embodiment of the invention. The document securing system 400 is, for example, performed by a computing device, such as client computer 701 or 702 shown in FIG. 7 below.

[0061] The document securing system 400 creates or obtains an electronic document 402 that is to be secured. The electronic document 402 is then supplied

to a securing engine 404. The securing engine 404 receives a designation of a classifier 406 to be associated with the electronic document 402. The classifier 406 refers to an accessor user list, and possibly other forms of access restriction. In one embodiment, the classifier 406 can be a label to a categorization of the electronic document with respect to a plurality of different types of content. Examples of classifiers include: External, Financial, Sales Forecast, Sales Quota, Press Release, Budget, Marketing Presentation, Marketing Planning, Engineering Planning, Engineering Project X, Engineering Specification, and Engineering Design. In addition, the securing engine 404 can receive a process-driven security policy 407 to be used to secure the electronic document 402. In one embodiment, the process-driven security policy 407 is chosen from a plurality of process-driven security policies based on the classifier 406. In another embodiment, the process-driven security policy 407 is made up of states, and each of the states correspond to one of the classifiers 406.

[0062] The securing engine 404 operates to produce a secured electronic document 408. The secured electronic document 408 includes an encrypted data portion 410 and a header portion 412. The encrypted data portion 410 is the electronic document 402 after having been encrypted. The encryption can result from the use of one or more keys and encryption algorithms. For stronger security, a hierarchy of encryption may be used. The header portion 412 is also referred to as encrypted security information, because the header portion 412 includes the encrypted security information as at least a substantial component of the header portion 412. The encrypted security information can include a classifier, access rules and at least one key (e.g., file key, private state key). The access rules and the keys utilized to encrypt the electronic document 402 depend on the state of the associated process-driven security policy 407 which is indicated by the classifier. Initially, the electronic document 402 is encrypted in accordance with an initial state of the process-driven security policy 407. Typically, one of the states of the process-driven security policy 407 is designated as its initial state.

[0063] Hence, if the encrypted security information is able to be decrypted, the file key is able to be retrieved from the header portion 412 and used to decrypt the encrypted data portion 410 of the secured electronic document 408, as will be discussed in more detail below with respect to FIG. 5C. However, the encrypted

security information in the header portion 412 is often secured through one or multiple layers of encryption, which can use various keys. These various keys are used to encrypt the security information. Typically, these various keys are managed by a server, but made available to client computers so that decryption can be performed locally. In one implementation, the encrypted security information within the header portion 412 can be decrypted if, and only if, the decrypting party has possession of both of the following: a group key (a private key for a group specified in the header), and a state key (a private key for the classifier specified in the header). As previously noted, the classifier is used to determine the state of the process-driven security policy 407.

[0064] Additional details on securing files or documents is provided in U. S. Patent Application No.: 10/159,537, filed May 5, 2002, and entitled "METHOD AND APPARATUS FOR SECURING DIGITAL ASSETS," which is hereby incorporated by reference.

[0065] FIG. 4B is a flow diagram of a document securing process 440 according to one embodiment of the invention. The document securing process 440 represents processing performed by a document securing system, such as the document securing system 400 illustrated in FIG. 4A.

[0066] The document securing process 440 initially opens or creates 442 an electronic document. Next, a decision 444 determines whether the electronic document is to be secured. When the decision 444 determines that the electronic document is not to be secured, then the electronic document is saved 446 in the normal course. Here, the electronic document is not secured but simply stored in a conventional fashion.

[0067] On the other hand, when the decision 444 determines that the electronic document is to be secured, then an initial policy reference for the electronic document is assigned 448. In one implementation, the policy reference is a pointer to an accessor user list. A classifier for an electronic document can be assigned in a variety of different ways. In one implementation, a user or creator of the electronic document is able to assign the classifier. For example, the user or creator of the electronic document might interact with a graphical user interface to select a classifier from a list of available classifiers.

[0068] After the policy reference is assigned 448, the electronic document is secured 450 in accordance with a process-driven security policy associated with the policy reference. Here, the electronic document is typically secured in accordance with the initial state of the process-driven security policy. Thereafter, the secured electronic document is saved 452. Following the operations 452 and 446, the document securing process 440 is complete and ends. The subsequent transitions to other states of the process-driven security policy is discussed below with reference to FIG. 6.

[0069] FIG. 4C is a detailed flow diagram of an encryption process 460 according to one embodiment of the invention. The encryption process 460 is, for example, processing suitable for being performed by the block 450 shown in FIG. 4B in which an electronic document is secured in accordance with a process-driven security policy.

[0070] According to the encryption process 460, a file key is obtained 462. In one implementation, the file key is a symmetric key used to encrypt and decrypt a data portion of a secured document. After the file key is obtained 462, the data portion of the electronic document is then encrypted 464 using at least the file key.

[0071] In one embodiment, each of the different states of the process-driven security policy would include a different public state key that would be used to encrypt documents being placed into such state. An initial state of the process-driven security policy associated with the policy reference is then determined 466. Next, a public state key associated with the initial state is obtained 468. Typically, the public state key is a public key of a public and private cryptography key pair that is to be utilized to encrypt documents associated with the initial state of the process-driven security policy. Once the public state key associated with the initial state has been obtained 468, the file key is encrypted 470 using the public state key. Thereafter, security information is attached 472 to the encrypted data portion. The security information, for example, can include the policy reference and the encrypted file key. For example, the policy reference can be used as a state indicator to identify the applicable state of the process-driven security policy.

[0072] In one embodiment, the policy reference has a key pair associated therewith. The file (document) security system (e.g., server) maintains the current

state of the process-driven security policy associated with the policy reference. The public key in this pair is used to encrypt the document and bind it with the process-driven security policy.

[0073] In this implementation, the electronic document has at least a data portion and a security information portion. The data portion is encrypted using at least the file key. In one embodiment, the electronic document can be encrypted many times over such that a plurality of different keys are needed to encrypt (and consequently to decrypt) the electronic document. In another embodiment, a key used to encrypt the electronic document can be encrypted many times over after being used to encrypt the electronic document. In other words, although the document securing process 440 refers to encryption of the data portion through use of the file key and then encryption of the file key through use of the public state key, it should be understood that additional keys can be used to directly encrypt the electronic document, or indirectly encrypt the electronic document by encrypting a key used to encrypt the electronic document. For example, the additional keys might include one or more of a classifier key, a user or group key, or a security clearance level key.

[0074] The security information is typically provided in a header (or header portion) of the electronic document. The header is thus typically attached to the encrypted data portion. The header together with the encrypted data portion represents a secured electronic document. Typically, the security information would include access rules, a policy reference (classifier), a private state key and at least one key (e.g., file key). The at least one key can be encrypted by a public state key that corresponds to the state, as well as possibly one or more other keys. The at least one key is often secured by encrypting either the at least one key itself, or the security information more generally, through use of one or more various other keys (e.g., group key, content type key, and/or clearance key).

[0075] FIG. 5A is a diagram of a document unsecuring system 500 according to one embodiment of the invention. The document unsecuring system 500 represents a counterpart to the document securing system 400 illustrated in FIG. 4A.

[0076] The document unsecuring system 500 cooperates to receive a secured electronic document 502. The secured electronic document typically includes an encrypted data portion 504 and a header 506. Often, but not necessarily, the header

506 is encrypted. The header 506 includes a policy reference and at least one key, e.g., a file key, that is needed to decrypt the encrypted data portion 504. The secured electronic document 502 is supplied to an unsecuring engine 508. The unsecuring engine 508 examines the header 506 of the secured electronic document 502 to determine the policy reference. The policy reference identifies a process-based security policy 510, or a state thereof, that governs the security of the secured document 502. The unsecuring engine 508 also receives at least that portion of the process-based security policy that pertains to the state of the secured electronic document 502. In other words, the unsecuring engine 508 needs the access restrictions for the current state of the process-driven security policy 510 to unsecure the secured electronic document 502, and thus gain access to its contents. The unsecuring engine 508 then evaluates whether the secured electronic document 502 is permitted to be accessed by the requestor, based on the access restrictions so retrieved. When the unsecuring engine 508 determines that the requestor is authorized to access the secured electronic document 502, then the unsecuring engine 508 can decrypt the encrypted data portion 504 of the secured electronic document 502 (and also eliminate at least significant portions of the header 506) to yield an electronic document 512 that is unsecured. In other words, the electronic document 512 is primarily (or exclusively) composed of the data portion of the encrypted data portion 504 after such has been decrypted. The decryption can involve the use of a number of keys (e.g., private keys) and decryption algorithms, one of such keys is the file key of the secured electronic document, and another of such keys is the private state key for the state of the secured electronic document.

[0077] FIGs. 5B and 5C are flow diagrams of a document access process 520 according to one embodiment of the invention. The document access process 520 operates to determine whether access to a particular document is permitted to a particular user (or group of users). The document access process 520 begins with a decision 522 that determines whether a request to access a secured electronic document has been received. When the decision 522 determines that such a request has not yet been received, the document access process 520 awaits such a request. Once the decision 522 determines that a request to access a secured electronic document has been received, the document access process 520 continues. In other words, the document access process 520 can be considered to

be invoked once a request to access a secured electronic document has been received.

[0078] In any case, once a request to access a secured electronic document has been received, a policy reference for the secured electronic document to be accessed is determined 524. In one embodiment, the security information portion of a secured electronic document contains the policy reference. Next, a process-driven security policy associated with the policy reference is determined 526. Then, the current state of the process-driven security policy for the secured electronic document is determined 528. In one embodiment, the policy reference (or other indicator) can indicate the current state of the state-based security policy. Next, access restriction are obtained 530 for the current state. Each of the different states of the process-driven security policy often has a different access restriction. Here, the state policy restrictions are those restrictions associated with the current state of a process-driven security policy.

[0079] Thereafter, a decision 542 determines whether the state policy restrictions are satisfied. In other words, the secured electronic document to be accessed is presently in the current state of the process-driven security policy. This current state has the access restriction associated therewith, that must be satisfied in order to gain access to the secured electronic document. Hence, the decision 542 determines whether the access restriction is satisfied by the requestor (e.g., user or group of users) seeking access to the secured electronic document. When the decision 542 determines that the access restriction is not satisfied, access to the secured electronic document is denied 544.

[0080] On the other hand, when the decision 542 determines that the access restriction has been satisfied, then a data portion of the secured electronic document is decrypted 546. Then, the data portion of the electronic document is returned 548 to the requestor. Following the block 548, as well as following the block 544, the document access process 520 ends.

[0081] FIG. 5D is a flow diagram of a decryption process 560 according to one embodiment of the invention. The decryption process 560 can, for example, pertain to detailed operations performed by the block 546 illustrated in FIG. 5C. In any event, the decryption process 560 initially obtains 562 an encrypted file key from the

security information portion of the secured electronic document. In addition, a private state key associated with the current state of the process-driven security policy for the secured electronic document is obtained 564. Normally, only authorized users would be able to gain access to the private state key. The private state key is the private key of the same public and private cryptography key pair that provided the public state key that was used to encrypt the file key. Then, the encrypted file key is decrypted 566 using the private state key. Thereafter, the data portion of the secured electronic document is decrypted 568 using at least the file key. Consequently, the data portion of the secured electronic document is decrypted and is in the "clear" and thus usable by the requestor. Following the block 568, the decryption process 560 is complete and ends.

[0082] FIG. 6 is a flow diagram of a transition process 600 according to one embodiment of the invention. The transition process 600 pertains to processing that can be utilized to transition between states of a process-driven security policy. More particularly, the transition process 600 is, for example, suitable for use as the processing performed by the block 208 illustrated in FIG. 2.

[0083] The transition process 600 initially obtains 602 an encrypted file key from the electronic document. Typically, the encrypted file key would be retrieved from the security information portion of the electronic document. Then, a private state key is obtained 604. Here, the private state key is associated with a previous state of a process-driven security policy that is imposed on the electronic document. After the private state key has been obtained 604, the encrypted file key is decrypted 606 using the private state key. At this point, the file key has been decrypted and could be used to decrypt the data portion of the electronic document. However, the file key is instead re-encrypted in accordance with a next (current) state. More specifically, a public state key is then obtained 608. The public state key is associated with the next state of the state-based security policy that is to be imposed on the electronic document. Then, using the public state key, the file key can be encrypted 610. Thereafter, the electronic document is re-saved 612. By re-saving 612 the electronic document, the security information portion of the electronic document is updated to include the new encrypted file key in accordance with the next state (or current state). Note that the data portion of the electronic document (which is secured by the file key) advantageously need not be decrypted in the transition process 600;

instead, the encryption of the file key is changed whenever a state transition occurs. Following the block 612, the transition process 600 is complete.

[0084] In one embodiment, to effect a state transition, the user only needs permission to effect the state transition. Additionally, users authorized to effect state changes with respect to a document, might be quite different from users authorized to access the document.

[0085] FIG. 7 shows a basic security system 700 in which the invention may be practiced in accordance with one embodiment thereof. The security system 700 may be employed in an enterprise or inter-enterprise environment. It includes a first server 706 (also referred to as a central server) providing centralized access management for the enterprise. The first server 706 can control restrictive access to files secured by the security system 700. To provide dependability, reliability and scalability of the system, one or more second servers 704 (also referred to as local servers, of which one is shown) may be employed to provide backup or distributed access management for users or client machines serviced locally. The server 704 is coupled to a network 708 and a network 710. For illustration purposes, there are two client machines 701 and 702 being serviced by the local server 704. Alternatively, one of the client machines 701 and 702 may be considered as a networked storage device.

[0086] Secured files may be stored in any one of the devices 701, 702, 704 and 706. When a user of the client machine 701 attempts to exchange a secured file with a remote destination 712 being used by an external user, one or more of the processing 300, 400, 500 and 600 discussed above are activated to ensure that the requested secure file is delivered without compromising the security imposed on the secured file.

[0087] According to one embodiment, a created document is caused to go through an encryption process that is preferably transparent to a user. In other words, the created document is encrypted or decrypted under the authoring application so that the user is not aware of the process. One or more keys, such as a state key, a user key and/or a content type key, can be used to retrieve a file key to decrypt an encrypted document. Typically, the user key is associated with an access privilege for the user or a group of users, and the content type key is

associated with the type of content of the created document. For a given secured document, only a user with proper access privileges can access the secured document.

[0088] In one setting, a secured document may be uploaded via the network 710 from the client computer 701 to a computing or storage device 702 that may serve as a central repository. Although not necessary, the network 710 can provide a private link between the computer 701 and the computing or storage device 702. Such link may be provided by an internal network in an enterprise or a secured communication protocol (e.g., VPN and HTTPS) over a public network (e.g., the Internet). Alternatively, such link may simply be provided by a TCP/IP link. As such, secured documents on the computer 702 may be remotely accessed.

[0089] In another setting, the computer 701 and the computing or storage device 702 are inseparable, in which case the computing or storage device 702 may be a local store to retain secured documents or receive secured network resources (e.g., dynamic Web contents, results of a database query, or a live multimedia feed). Regardless of where the secured documents or secured resources are actually located, a user, with proper access privileges, can access the secured documents or resources from the client computer 701 or the computing or storage device 702 using an application (e.g., Microsoft Internet Explorer, Microsoft Word or Adobe Acrobat Reader).

[0090] Accordingly, respective local modules in local servers, in coordination with the central server, form a distributed mechanism to provide distributed access control enforcement. Such distributed access control enforcement ensures the dependability, reliability and scalability of centralized access control management undertaken by the central server for an entire enterprise or a business location.

[0091] FIG. 8 shows an exemplary data structure 820 of a secured file that may be used in one embodiment of the invention. The data structure 820 includes two portions: a header (or header portion) 822 and encrypted data (or an encrypted data portion) 824. The header 822 can be generated in accordance with a security template associated with a data store and thus provides restrictive access to the data portion 824 which is an encrypted version of a plain file. Optionally, the data structure 820 may also include an error-checking portion 825 that stores one or more

error-checking codes, for example, a separate error-checking code for each block of encrypted data 824. These error-checking codes may also be associated with a Cyclical Redundancy Check (CRC) for the header 822 and/or the encrypted data 824. The header 822 includes a flag bit or signature 827 and security information 826 that is in accordance with the security template for the store. According to one embodiment, the security information 826 is encrypted and can be decrypted with a user key associated with an authenticated user (or requestor).

[0092] The security information 826 can vary depending upon implementation. However, as shown in FIG. 8, the security information 826 includes a user identifier (ID) 828, access policy (access rules) 829, a file key 830, a classifier 831 and other information 832. Although multiple user identifiers may be used, a user identifier 828 is used to identify a user or a group that is permitted to access the secured file. The access rules 829 provide restrictive access to the encrypted data portion 824. The file key 830 is a cipher key that, once obtained, can be used to decrypt the encrypted data portion 824 and thus, in general, is protected. In one implementation of the data structure 820, the file key 830 is encrypted in conjunction with the access rules 829. In another implementation of the data structure 820, the file key 830 is encrypted with a private state key and further protected by the access rules 829. The other information 832 is an additional space for other information to be stored within the security information 826. For example, the other information 832 may be used to include other information facilitating secure access to the secured file, such as version number or author identifier.

[0093] The invention is preferably implemented by software or a combination of hardware and software, but can also be implemented in hardware. The invention can also be embodied as computer readable code on a computer readable medium. The computer readable medium is any data storage device that can store data which can thereafter be read by a computer system. Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves. The computer readable medium can also be distributed over network-coupled computer systems so that the computer readable code is stored and executed in a distributed fashion.

[0094] The various embodiments, implementations and features of the invention noted above can be combined in various ways or used separately. Those skilled in

the art will understand from the description that the invention can be equally applied to or used in various other settings with respect to different combinations, embodiments, implementations or features as provided in the description herein.

[0095] The invention may be practiced in two broad approaches: one, where document move asynchronously through a persistent workflow (here, the state changes are typically triggered by the users); and two, where documents move synchronously through a single-use workflow, a plurality of which however can be initiated from a workflow template (here, the state changes are typically due to administrator central command). The two approaches may be combined for use in a single enterprise. State changes due to external events may occur with both approaches.

[0096] The advantages of the invention are numerous. Different embodiments or implementations may yield one or more of the following advantages. One advantage of the invention is that file security systems are able to automatically enforce process-driven security policies on files (e.g., documents). The automatic nature of the enforcement of the process-driven security policies alleviates otherwise excessive burdens on an administrator. Another advantage of the invention is that changing of the security policies for files (e.g., documents) in accordance with a process allows greater flexibility in utilizing security policies. Still another advantage of the invention is that the process-driven security policies can be enforced centrally or locally. Still another advantage is that a workflow ordered through a centralized document management system (DMS) may be extended to a plurality of documents stored in a distributed fashion, thereby allowing a system administrator to use the well-known DMS interface.

[0097] The foregoing description of embodiments is illustrative of various aspects/embodiments of the present invention. Various modifications to the invention can be made to the preferred embodiments by those skilled in the art without departing from the true spirit and scope of the invention as defined by the appended claims. Accordingly, the scope of the present invention is defined by the appended claims rather than the foregoing description of embodiments.

What is claimed is: